UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/710,541	11/09/2000	Christopher Paul Carroll	99-956	5815

32127 7590 03/24/2006

VERIZON CORPORATE SERVICES GROUP INC.
C/O CHRISTIAN R. ANDERSEN
600 HIDDEN RIDGE DRIVE
MAILCODE HQE03H14
IRVING, TX 75038

EXAMINER	
NOBAHAR, ABDULHAKIM	
ART UNIT	**PAPER NUMBER**
2132	

DATE MAILED: 03/24/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/710,541	CARROLL, CHRISTOPHER PAUL	
	Examiner	Art Unit	
	Abdulhakim Nobahar	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 December 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _____ is/are rejected.

7)☒ Claim(s) *2-4,13,14,23 and 29* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Response to Arguments

1. This communication is in response to applicant's amendment received on December 29, 2005.

2. Applicant's arguments, see pages 10-18 of Remarks, filed December 29, 2005, with respect to the rejection(s) of claims 1, 12, 19, 24 and 32 under 35 USC 103(a) have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made as follows:

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 5-12, 15-22, 24-28 and 30-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Aura (6,711,400 B1) in view of applicant admitted prior art hereinafter referred to as APA.

Aura discloses an authentication method for a telecommunication system that a mobile subscriber is authenticated to both visiting and home networks and vice versa

(see, for example, abstract), i.e., the authenticity of the subscriber's identity is verified by the networks and the subscriber checks the authenticity of the networks' identities.

Claims 1, 5, 6 and 19

Aura discloses:

storing a key at the service network (see, for example, col. 3, lines 1-4; col. 7, lines 7-12, where the visited network VPLMN corresponds to the recited service network);

transmitting information to the station from the service network that enables the station to compute the key stored at the service network (see, for example, col. 7, lines 13-25; Figs. 2-4, where the MS receives information from VPLMN to compute Kc);

receiving a request for service at the service network from the station (see, for example, col. 6, lines 16-21; Figs. 4-5);

transmitting information to the station that forms a part of a verification computation enabling the station to authenticate the service network (col. 7, lines 13-25 and Fig. 4, where RAND1 and RAND2 form information in the computations used by algorithms H1, H2, and H3 that are used by the mobile subscriber to authenticate the visited network.)

determining at the home environment network a cryptographic primitive offered to the home environment by the service network (Fig. 4, where the VPLMN transmit IMSI and RAND1 to the HLR/AUC to compute the cryptographic primitive SRES1, SRESD' and Kc); and

based on the determined cryptographic primitive, transmitting to the service network at least one vector of authentication information corresponding to a particular station (see, for example, Fig. 4, where RAND2 and SRES1 which are corresponding to an MS with Ki are transmitted to the VPLMN).

Aura, however, does not expressly disclose:

adjusting a verification value at each usage of the key; and

transmitting, from the service network to the station, information corresponding to the verification value.

APA discloses that the mobile station (MS) and the home environment (HE) network keep track of counters SQN_{MS} and SQN_{HE} and whenever HE generates an authentication vector (corresponding to the recited adjusting a verification value at each usage of the key), SQN_{HE} is incremented. The MS authenticates the serving network (SN) based on these sequence numbers (see, for example, page 4 of the specification, lines 3-10). APA further discloses that the SN sends sequence number related information such as RAND(i) and AUTN(i) to MS (see, for example, page 4 of the specification, lines 20-32). The MS after verifying AUTN(i) and computing RAND(i) compares SQN(i) with SQN_{MS} to authenticate NS.

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to deploy a counter associated to a key usage as taught in APA in the method of Aura because it would provide a means for a mobile station to authenticate a visited network (APA, page 4, lines 3-5).

Claim 7

Aura discloses:

the station comprises a cellular phone; and

the service network and home environment networks comprise cellular networks (see, for example, col. 1, line 49-col. 2, line 3 and Fig. 1).

Claim 8

Aura discloses:

using the key to compute a cipher key for encrypting communication between the service network and the station (see, for example, Fig. 3, where the key DCK is calculated for encrypting communication between the visited network and the mobile station at stages 327 and 315).

Claim 9

Aura discloses:

negotiating use of a cryptographic primitive between the service network and the home environment network (see, for example, Fig. 3, where the home network at stage 302 uses the primitive TA11 for calculation of KS and the service network BS uses primitive TA12 at stage 312 to calculate DCK1 which also calculated by MS at stage 323 using TA12. The calculation of DCK1 at MS is dependent upon the value KS. This implies that the home network is aware of the primitives used at the BS and based on this knowledge the home network transmits the required authentication vector to the

visiting network to be used by a specific primitive which corresponds to the recited negotiating use of a cryptographic primitive...).

Claim 10

Aura discloses:

transmitting a challenge to the station (see, for example, Fig. 4, where the challenge RAND2 at stage 406 is sent to the MS);

receiving a challenge response from the station (see, for example, Fig. 4, where the SRES2 at stage 409 is received); and

comparing the received challenge response with an expected response (see, for example, Fig. 4, stage 409).

Claim 11

Aura discloses:

computing the key stored by the service network at the station (see, for example, Fig. 4, stage 407, the key Kc is calculated and also stored at the VPLMN).

Aura, however, does not expressly disclose:

receiving the information indicating the value corresponding to key usage at the station; and

comparing the received value with a value corresponding to key usage maintained by the station.

APA discloses that the mobile station (MS) and the home environment (HE) network keep track of counters SQN_{MS} and SQN_{HE} and whenever HE generates an authentication vector (corresponding to the recited usage of the key), SQN_{HE} is incremented. The MS authenticates the serving network (SN) based on these sequence numbers (see, for example, page 4 of the specification, lines 3-10). APA further discloses that the SN sends sequence number related information such as RAND(i) and AUTN(i) to MS (see, for example, page 4 of the specification, lines 20-32). The MS after verifying AUTN(i) and computing RAND(i) compares SQN(i) with SQN_{MS} to authenticate NS.

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to deploy a counter associated to a key usage as taught in APA in the method of Aura because it would provide a means for a mobile station to authenticate a visited network (APA, page 4, lines 3-5).

Claim 12

Aura discloses:

A method for use in authenticating a service network to a station, the station having a home environment network, the method comprising:

receiving information at the station from the service network (see, for example, Fig. 4, RAND2 and SRES1 at stage 407; col. 7, lines 13-46);

computing a key based on the information received at the station from the service network, the computed key also being stored by the service network (see, for example, Fig. 4, Kc at stages 407 and 405; col. 7, lines 9-46);

Aura, however, does not expressly disclose:

maintaining an indicator of key usage at the station;

receiving at the station an indicator of key usage maintained by the service network; and

comparing the key usage indicator maintained by the service network with the key usage indicator maintained by the station.

APA discloses that the mobile station (MS) and the home environment (HE) network keep track of counters SQN_{MS} and SQN_{HE} and whenever HE generates an authentication vector (corresponding to the recited an indicator of key usage), SQN_{HE} is incremented. The MS authenticates the serving network (SN) based on these sequence numbers (see, for example, page 4 of the specification, lines 3-10). APA further discloses that the SN sends sequence number related information such as RAND(i) and AUTN(i) to MS (see, for example, page 4 of the specification, lines 20-32). The MS after verifying AUTN(i) and computing RAND(i) compares SQN(i) with SQN_{MS} to authenticate NS.

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to deploy a counter associated to a key usage as taught in APA in the method of Aura because it would provide a means for a mobile station to authenticate a visited network (APA, page 4, lines 3-5).

Claim 15

Aura discloses:

the station comprises a cellular phone; and

the service network and home environment networks comprise cellular networks (see, for example, col. 1, line 49-col. 2, line 3 and Fig. 1).

Claim 16

Aura discloses:

using the key to compute a cipher key for encrypting communication between the service network and the station (see, for example, Fig. 3, where the key DCK is calculated for encrypting communication between the visited network and the mobile station at stages 327 and 315).

Claim 17

Aura discloses:

receiving a challenge from the service network (see, for example, Fig. 4, where the challenge RAND2 at stage 407 is received by MS);

determining a challenge response (see, for example, Fig. 4, where at stage 407 SRES2 is computed); and

transmitting the challenge response to the service network (see, for example, Fig. 4, where SRES2 is transmitted to VPLMN at stage 409).

Claim 18

Raith discloses the use of a counter in association with the usage of an encryption key by a mobile station (see, for example, col. 8, lines 54-67; col. 21, line 22-col. 22, line 37).

Claim 20

Aura discloses:

receiving identification of the cryptographic primitive from the service network (see, for example, Fig. 4, where RAND2 received by MS at stage 407 which is generated by the home network using a hash function at stage 404).

Claim 21

Aura discloses:

identification comprises a value of a MODE field (see, for example, Fig. 4, where SRES1 which is the product of a hash value that represents a value corresponding to the recited MODE field).

Claim 22

Aura discloses:

the vector authentication information comprises an indication of an authentication vector sequence number maintained by the home environment network. (see, for example, Fig. 4, where RAND2, SRES1, SRES2' and Kc are the vector of authentication information received by the visited network from the home network and these information are based on Ki which represents the encryption key for the ith mobile station that corresponds to the ith position of a vector in the sequence a I's values of vector information)

Claim 24

This claim is rejected as applied to the like elements of the claims 1 and 19 as stated above and further the following:

Aura discloses:

storing different sets of cryptographic information for the different respective service networks (Fig. 4, where MS stores SRES1', SRES2 and Kc to communicate with a particular VPLMN);

selecting one of the sets of cryptographic information for one of the service networks; and

using the one selected set of cryptographic information to communicate with the one service network (Fig. 4, where MS selects Kc for communication with the VPLMN after bilateral authentication).

Aura also discloses that a cryptographic key is computed each time a MS is establishing communication with a visited network (Fig. 4, where the Kc is calculated by both MS and the AUC and stored at the visited network).

Claim 25

Aura discloses:

the sets of cryptographic information comprise a key shared by the station and the service network (see, for example, Fig. 3, where the cryptographic key DCK is used by both MS and the visiting network for communicating with each other).

Claim 26

Aura discloses:

computing the key shared by the station and the service network based on information received from the service network (see, for example, Fig. 3, where at stage 327 the cryptographic key DCK is computed based on the DCK1 and DCK2 that are in turn computed based on KS and KS'. The KS and KS' are calculated based on RS received from the service network. Thus, DCK is based on the RS).

Claims 27 and 28

APA discloses that the MS keeps SQN_{MS}, which is a sequence number and an indicator of key usage along with other cryptographic information (APA, page 4, lines 3-5 and Fig. 3/15).

Claim 30

Aura discloses:

using the selected set of cryptographic information comprises using the selected set cryptographic information to authenticate the service network (see, for example, Fig. 4, where SRES1' is selected by the MS to authenticate the visited network at stage 408).

Claim 31

Aura discloses:

using the selected set cryptographic information comprises using the selected set of cryptographic information in encrypting communication between the station and the service network (see, for example, Fig. 4, where the cryptographic key Kc is selected for encrypting communication between the station and the service network).

Claim 32

This claim is rejected as applied to the like elements of claims 1 and 19 as stated above and further the following:

Aura discloses:

determining whether the home environment and the service network share a cryptographic primitive offered by the service network (col. 2, lines 15-18, where the algorithms that are used in the process of authentication are located in both authentication center that corresponds to the recited service network and in the subscriber unit that corresponds to the home environment; col. 2, lines 26-36 where the hash functions are provided to a subscriber by a center that corresponds to the recited service network; Fig. 4, where the MS uses the same hash functions that are used in the authentication center of the visited network in order to compute responses for the visited network; see also col. 4, lines 9-55);

computing a shared secret key (SSK) (see, for example, Fig. 4, where the cryptographic key Kc is computed at the visited network's AUC);

transmitting information from the service network to the station that enables the station to compute the SSK (see, for example, Fig. 4, where RAND2 and SRES1 are transmitted to the MS by the visited network to calculate shared Kc).

Aura, however, does not expressly disclose that if it is determined that the home and visited networks do not share a cryptographic primitive, the 3GPP AKA is used for authentication operation between the mobile station and the visiting network.

APA teaches an authentication method that a service network and a mobile station authenticate each other using 3GPP AKA technology in the absence of a shared a cryptographic primitive (i.e., a shared algorithm) (see page 3, lines 9-16; page 4, lines 3-33)

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to implement the process of determining to use a 3GPP AKA technology or a shared cryptographic primitive as taught in APA in the system of Aura because it would enhance the process of authentication between a mobile station and a visited network (page 3, lines 11-14).

Allowable Subject Matter

Claims 2-4, 13-14, 23 and 29 objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

US Patent No. 5239294 A to Flanders et al.

US Patent No. 5506905 A to Morkowski et al.

US Patent No. 6243811 B1 to Patel.

US Patent No. 6574730 B1 to Bissell et al.

US Patent Pub. No. 20030033522 A1 to Bilgic et al.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Abdulhakim Nobahar whose telephone number is 571-272-3808. The examiner can normally be reached on M-T 8-6.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Abdulhakim Nobahar
Examiner
Art Unit 2132 A.N.

March 15, 2006

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100